

INFORMATION SECURITY POLICY

R Bostock Enterprises B.V.
Curacao Gaming Authority (CGA) Licensed

Document Information	
Approving Official(s):	Pulkit Totla
Responsible Office:	IT Department / Compliance Department
Effective Date:	March 3, 2026
Next Review Date:	March 3, 2027

1. Policy Statement

R Bostock Enterprises B.V. is committed to protecting the confidentiality, integrity, and availability of all information assets. Under CGA license, the company maintains robust information security controls to protect player data, financial records, and business operations. This Information Security Policy establishes the foundation for a comprehensive security program that addresses current and emerging threats, ensures regulatory compliance, and protects the interests of the company, its employees, customers, and stakeholders.

2. Purpose

To establish an information security framework that protects the company and its customers from cyber threats, data breaches, and unauthorized access, in compliance with CGA requirements, Curacao data protection laws, and industry best practices. This policy defines the security standards, controls, and procedures that all personnel must follow.

3. Audience

This policy applies to all employees, contractors, third-party service providers, consultants, and any persons with access to company information systems and data. All recipients of this policy are responsible for understanding and complying with its requirements.

4. Definitions

- **Information Asset:** Any data, system, or resource that holds value to the organization.
- **Confidential Information:** Information restricted to authorized personnel only.
- **Personal Data:** Information relating to identified or identifiable individuals.
- **Data Breach:** Unauthorized access, disclosure, or loss of data.
- **Access Control:** Mechanisms restricting system and data access to authorized users.

- **Encryption:** Conversion of data into coded form to prevent unauthorized access.
- **Firewall:** Network security device filtering traffic between networks.
- **Intrusion Detection System (IDS):** System monitoring networks for malicious activities.
- **Penetration Testing:** Authorized security testing simulating attacks on systems.
- **Vulnerability Assessment:** Systematic identification of security weaknesses.
- **Incident Response:** Coordinated actions to manage security incidents.
- **Business Continuity:** Processes enabling operations during disruptions.
- **Disaster Recovery:** Procedures restoring IT systems after disasters.
- **Multi-Factor Authentication (MFA):** Authentication requiring multiple verification methods.
- **Data Classification:** Categorization of data based on sensitivity and protection needs.

5. Policy Implementation

5.1 Information Classification

- The organization classifies all information into four levels based on sensitivity and criticality:
 - **Public:** Information suitable for public disclosure. Minimal protection required. Includes marketing materials and public announcements.
 - **Internal:** Information for internal use only. Moderate protection. Includes internal policies, meeting notes, and routine communications.
 - **Confidential:** Sensitive information requiring significant protection. Includes financial data, proprietary processes, and strategic plans.
 - **Restricted:** Highly sensitive information requiring maximum protection. Includes player personal data, financial records, passwords, and authentication credentials.

All player personal data and financial data must be classified as 'Restricted'. All information must be labeled appropriately according to classification level.

5.2 Access Control

- Role-based access control (RBAC) implemented for all systems.
- Principle of least privilege: users granted minimum permissions necessary.
- Multi-factor authentication (MFA) mandatory for all systems, particularly for administrative and sensitive data access.
- Password policy: Minimum 12 characters with complexity requirements (uppercase, lowercase, numbers, special characters).
- Password rotation every 90 days; last 12 passwords cannot be reused.
- Account lockout after 5 failed authentication attempts; 30-minute lockout duration.
- Quarterly access reviews to ensure continued appropriateness of permissions.
- Immediate access revocation upon employment termination or role change.
- Privileged Access Management (PAM) system for administrative accounts.

5.3 Data Protection and Privacy

Encryption Standards: AES-256 for data at rest; TLS 1.2 or higher for data in transit.

Data Center Requirements: Player data must be stored in Tier-IV certified data center located in Curacao (CGA requirement).

- Data minimization principles: collect and retain only necessary data.
- Data retention: Personal and financial data retained for 5 years after end of business relationship, then securely disposed.
- Secure data disposal procedures: Shredding of documents, degaussing or destruction of magnetic media, cryptographic erasure of digital media.
- Privacy Impact Assessments (PIA) required for new systems or processes handling personal data.
- Cookie policy and informed consent management for all user data collection.

5.4 Network Security

- Firewall configuration and management following principle of least privilege.
- Intrusion Detection/Prevention Systems (IDS/IPS) deployed and monitored continuously.
- Network segmentation: Production, development, and DMZ environments isolated.
- VPN (Virtual Private Network) required for all remote access.
- Regular network vulnerability scanning (at least monthly).
- DDoS (Distributed Denial of Service) protection measures implemented.
- Wireless network security: WPA3 encryption, strong authentication, regular monitoring.

5.5 Endpoint Security

- Anti-malware software deployed on all endpoints with real-time scanning.
- Endpoint Detection and Response (EDR) solution for threat detection and response.
- Full disk encryption on all laptops and mobile devices.
- Mobile Device Management (MDM) for company-issued mobile devices.
- BYOD (Bring Your Own Device) policy: Restricted to non-sensitive work; separate profile required.
- USB and removable media controls: Disabled by default, enabled only with authorization.
- White Room environment for customer-facing departments: No personal devices, cameras, or removable media permitted.

5.6 Application Security

- Secure Software Development Lifecycle (SSDLC) implemented for all application development.
- Code review required for all production code before deployment.
- OWASP Top 10 compliance mandatory for all web applications.
- Regular application vulnerability testing (at least annually and after significant changes).
- Third-party software vetting process including license and security review.
- Patch management procedures: Critical patches within 24 hours, High within 7 days, Medium within 30 days.

5.7 Incident Response

Incident Classification:

- **P1 (Critical):** System outage, active data breach, widespread malware infection.
- **P2 (High):** Significant system degradation, potential data exposure.
- **P3 (Medium):** Minor data loss, isolated system issue, failed access attempt.
- **P4 (Low):** Informational alerts, no operational impact.
- Incident Response Process:
 - Detection
 - Containment
 - Eradication
 - Recovery
 - Lessons Learned
- Data Breach Notification: CGA notification required within 72 hours; affected players notified promptly.
- Forensic investigation procedures for all security incidents.
- Post-incident review and remediation to prevent recurrence.

5.8 Business Continuity and Disaster Recovery

- Business Impact Analysis (BIA) identifying critical systems and data.
- Recovery Time Objective (RTO): Maximum 4 hours for critical systems.
- Recovery Point Objective (RPO): Maximum 1 hour data loss.
- Backup procedures: Daily incremental backups, weekly full backups, off-site replication.
- Disaster Recovery (DR) site established with failover capabilities.
- Annual BCP/DR testing with documented results.
- Communication plan for stakeholders during major incidents.

5.9 Physical Security

- Office access controls using swipe cards or key fobs.
- CCTV monitoring of entry/exit points and sensitive areas.
- Visitor management with sign-in/sign-out procedures and escort requirements.
- Clean desk policy: No sensitive documents left unattended; secure storage when not in use.
- Secure disposal of physical documents (shredding) and media (degaussing/destruction).
- Restricted areas for server rooms and communications equipment with enhanced access controls.
- White Room requirements for sensitive departments: No removable media, cameras, or recording devices.

5.10 Third-Party Security

- Security requirements incorporated into all vendor contracts.
- Vendor risk assessments before engagement and annually thereafter.

- Data Processing Agreements (DPA) for vendors processing personal data.
- Regular vendor security reviews and compliance monitoring.
- Right to audit clause in vendor contracts.
- Incident notification requirements (within 24 hours for security incidents).

5.11 Security Awareness Training

- Mandatory security training at employee induction.
- Annual refresher training for all personnel.
- Quarterly phishing simulation exercises with metrics tracking.
- Specialized training for IT and development staff (secure coding, incident response, etc.).
- Record keeping of all training completion with dates.
- Targeted training for high-risk roles (data handlers, administrators).

5.12 Compliance and Audit

- Annual security audits (both internal and external).
- Penetration testing at least annually and after significant system changes.
- Quarterly vulnerability assessments of all systems.
- Compliance monitoring with CGA technical requirements and regulations.
- Security metrics and KPI reporting to management quarterly.
- Audit findings tracked and remediated with timelines.

5.13 Acceptable Use Policy

Permitted Use: Company systems intended for business purposes.

Internet Usage: Limited personal use acceptable; no illegal or inappropriate content.

Email Security: Be cautious of phishing; do not forward confidential information without authorization.

Social Media: No disclosure of company information; maintain professional standards.

Prohibited Activities: Hacking, malware distribution, data theft, unauthorized access, pornography, gambling, harassment.

Company Device Monitoring: Organization reserves right to monitor company devices for security and compliance purposes.

6. Compliance and Consequences of Non-Compliance

- Non-compliance with this Information Security Policy may result in disciplinary action up to and including termination of employment. Additionally, violations may result in:
 - Criminal prosecution for data theft, hacking, or unauthorized access.
 - Civil liability and monetary damages.
 - Regulatory penalties and fines from CGA and data protection authorities.

- Reputational damage to the organization.

7. Related Information

- CGA Technical Requirements
- ISO/IEC 27001:2022 Information Security Management
- OWASP Security Standards
- AML/CTF Policy
- KYC (Know Your Customer) Policy
- Curacao Data Protection Legislation
- Incident Response Plan
- Business Continuity Plan
- Disaster Recovery Plan

8. Contact Information

Questions regarding this policy should be directed to:

- IT Department / Chief Information Security Officer
- Compliance Department / Compliance Officer
- Email: security@rbostock.com
- Phone: +599 (Curacao) - Available during business hours

9. Policy History

Version	Date	Author/Approver	Change Description
1.0	March 3, 2026	Pulkit Totla	New Policy - Initial Release

Signature and Approval

Information Security Policy
R Bostock Enterprises B.V.



Pulkit Totla

Date: March 3, 2026

*This Information Security Policy is confidential and intended only for authorized personnel of R Bostock Enterprises B.V.
Unauthorized distribution is prohibited.*